

HIGHLY EFFICIENT IMAGE STEGANOGRAPHY USING HAAR DWT FOR HIDING MISCELLANEOUS DATA

Hamad A. Al-Korbi¹, Ali Al-Ataby², Majid A. Al-Tae³ and Waleed Al-Nuaimy⁴

Department of Electrical Engineering and Electronics

University of Liverpool, Liverpool, UK

hamad.a.qa@ieee.org¹; {aliataby², altaeem³, wax⁴}@liv.ac.uk

(Received: 15-Dec.-2015, Revised: 22-Jan.-2016, Accepted: 31-Jan.-2016)

ABSTRACT

Protecting private data exchanged over the Internet and controlling access to this data have become a growing privacy and confidentiality concern. Digital image steganography helps conceal private data within a cover image to obtain a new image, practically indistinguishable from the original, in such a way that unauthorized individuals cannot detect the presence of the concealed data in the new cover. Capacity size of the cover image and imperceptibility are therefore considered critical requirements to assess the performance of steganography algorithms. This paper presents a highly efficient steganography algorithm that is capable of hiding a large size of miscellaneous data (text files, binary images, coloured images or a combination of these data types) in a single cover image using Haar Wavelet transform. Details of the proposed embedding and extraction algorithms for different data types are presented and discussed. The performance of the proposed steganography method is assessed in terms of the capacity of the cover image, imperceptibility and robustness. The obtained experimental results and observations demonstrated that the developed algorithms are highly efficient in terms of the capacity size of the cover image while maintaining a relatively low mean square error (MSE), high peak signal-to-noise ratio (PSNR) and a reasonable robustness against various attacks.

KEYWORDS

Data hiding, Haar Wavelet transform, Information security, LSB, MSE, Pseudo random number, PSNR, Robustness, Steganography.

1. INTRODUCTION

With the worldwide growth of Internet users, security and confidentiality have become a prime importance to protect personal and sensitive data from unauthorized access. Numerous data hiding methods have been reported in the literature to increase the level of information security. Of these, cryptography [1]–[4], steganography [5]–[7] and watermarking [8]–[10] are the most common methods in practice today. Searching Google for cryptography, steganography and watermarking has recently returned 3.9, 0.519 and 0.743 million results, respectively. This provides evidence for the growing importance of information hiding. Unlike cryptography in which the sender converts plaintext to cipher-text (or vice versa) by using an encryption/decryption key, steganography and watermarking are about embedding data within another object known as a cover by tweaking its properties. Steganography and watermarking however differ in their goals, implementations, applications, size of embedded data and robustness requirements.

The term steganography was extracted from a Greek word, meaning covered writing, where ‘stegano’ means ‘cover’, while ‘graphos’ is known as ‘writing’ in English. Its main goal is to

hide a message m in a cover data c , to obtain new data c' , practically indistinguishable from c , by people, in such away that unauthorized individuals cannot *detect the presence of m* in c' . In contrast, the main goal of watermarking is to hide a message m in a cover data c , to obtain new data c' , practically visible or invisible, in such a way that unauthorized individuals cannot *remove or replace m* in c' . Thus, steganography methods usually do not need to provide strong security against removal or modification of the hidden message, while watermarking methods need to be robust enough against attempts to remove or modify the hidden message [8]–[10]. Furthermore, steganography is typically used to conceal a message in one-to-one communications, while watermarking is used whenever the cover-data is available to many parties who are aware of the presence of the hidden data [4].

Popular applications of watermarking are copyright protection and ownership verifications of digital data by embedding copyright statements (visible or invisible), monitoring data transmission in order to control royalty payments or simply tracking the distribution to localize the data for marketing [4]. Image steganography applications on the other hand follow one general principle of hiding a large-size secret data in a single cover image that is exchanged between the communicating parties. The capacity size of the cover image (c) and imperceptibility of the stego image (c') are therefore considered the main critical requirements for steganography.

Peak signal-to-noise ratio (PSNR) and the mean square error (MSE) have been widely used metrics to evaluate the imperceptibility of stego images. In [11], the authors suggested that one secret image in the spatial domain can be concealed within the cover image using the least significant bit (LSB) technique. Random pixels of the cover image will be selected in order to modify their LSB with the most significant bits (MSB) of the secret image or private text; hence the stego image is formed. However, this method provides low PSNR, low MSE as well as low level of the overall security. Another model proposed that an image could be hidden into another image using pixel-value differencing [12]. The PSNR and MSE values were equal to 41.79 dB and 2.07, respectively. Moreover, It has been suggested that discrete cosine transform (DCT) combined with LSB method can be used for enhanced steganography technique [13]. The idea of this method is to convert the images into the frequency domain by applying DCT, and then the secret data will be hidden in the LSB of the DCT coefficients. However, in this method, PSNR value was about 38 dB.

In an effort to develop the system, a steganography algorithm based on the Wavelet transform has also been introduced. In this method, both secret and cover images will be converted from the spatial domain into frequency domain using Wavelet transform. Then, the secret image will be concealed within the cover image using LSB method. The inverse of the Wavelet transform is applied in order to obtain the cover image in the spatial domain. Efficient PSNR and MSE were achieved [5], [7], [14]–[15]. Another method was also developed where both cover and secret images will be decomposed into their three-colour layers R, G and B [16]. Using discrete wavelet transform (DWT), each layer is divided into four levels. After that, alpha combination method is applied to conceal each layer of the secret image. The PSNR value of this method was 29 dB.

Steganography system performance can be improved by applying both DWT and DCT [17]. The cover image can be sub-divided into four sub-bands using DWT and the DCT is applied to the HH sub-band. Secret image is dispersed into HH using session key and sequences pseudo random. Outcome PSNR of this method is 27.39 dB. Moreover, it was suggested that Wavelet transform and genetic algorithm can be used to achieve high capacity image steganography [18]. It was argued that the genetic algorithm based mapping could be used to embed the secret information into the coefficients of the DWT in 4×4 blocks cover image. A high value of PSNR was achieved, along with the capacity; both are equal to 45.2 dB and 50%, respectively.

High capacity data hiding using LSB steganography and encryption is a new field of steganography. This technique using LSB and encryption aimed to have high capacity as well as an acceptable level of the overall security [19]. Furthermore, a new model was developed, where a robust and highly secure steganography algorithm using dual Wavelet and blending mode was applied [20]. Further research was carried out on steganography techniques in order to increase the capacity as well as the PSNR using DWT and Arnold Transform [21]. The capacity and the PSNR were equal to 75% and about 50 dB, respectively. Another steganography technique was also proposed in [22], using DWT and Huffman coding. The achieved PSNR and capacity from this technique were 54.93 dB and 64.5%, respectively. In conclusion, the performance of steganography techniques has been a trade-off among capacity, security, robustness and distortion.

In [23], the authors reported a steganography technique based on the discrete wavelet transform. This technique was capable of hiding a secret message and a small-size image into a large-size image. Another steganography method was also reported in [15] that was capable of hiding one secret image within another single image. However, most of the previously reported steganography techniques support hiding size images or text messages or a combination of both.

Wavelet transform-based steganography techniques are usually criticized because of the inherent complexity and cost of the incorporated algorithms, in such a way that the trade-off between complexity and performance is not justified. In this paper, we present a more efficient steganography technique that extends a previously reported work by the authors in [5] based on Haar wavelet transform. The proposed technique allows hiding any combination of secret images (black and white (B&W) or coloured) and large secret text files can be concealed within a single cover image. All these types of private data can be concealed in a single stego image of a size of $512 \times 512 \times 3$ pixels. In addition, the stego image is formed to be always equal to the cover image.

The remaining of this paper is organized as follows. Background information on the wavelet transform, least significant bit (LSB) and pseudo random number techniques that are adopted in the proposed steganography are presented in Section 2. Details of the proposed embedding and extraction algorithms are given in Section 3. Data hiding scenarios for different combinations of data types are discussed in Section 4. Performance metrics that are used to evaluate the proposed steganography are presented in Section 5. The obtained evaluation results are presented and discussed in Section 6. Finally, the work is concluded in Section 7.

2. BACKGROUND

This section provides theoretical background on wavelet transform, least significant bit (LSB) and pseudo random number techniques.

2.1 Haar DWT

One of the most developed transforms that can be used to transform a signal from the spatial to the frequency domain and vice versa is the Wavelet transform. The Wavelet transform, and other related transforms, can be considered a second generation of transforms. Wavelets are defined as oscillations of short waves that decay rapidly over time [24]. Moreover, they have an enormous number of applications that can be implemented in various fields such as signal processing, data compressing, fingerprint verification, smoothing, image de-noising and speech recognition. It has been reported that the Wavelet transform can be applied to the steganography technique in order to increase the capacity as well as the robustness [25]. One of the Wavelet transform families known as “Haar” has been implemented in this work. It converts an image from spatial domain to frequency domain by applying horizontal and vertical operations, respectively.

The Haar DWT is used in the proposed steganography technique. It is the simplest transform in wavelet mathematics, because it uses square pulses to approximate the original function. It is used to convert the cover image into four sub-bands that are approximation, vertical, horizontal and diagonal coefficients, which represent low-low, high-low, low-high and high-high frequencies, respectively. Approximation coefficients will not be used to conceal secret information, since human eyes are very sensitive to small changes in the low-low frequency. However, the rest of the coefficients contain high frequencies, thus secret data will be corrected and concealed within these bands by the use of both least significant bit and pseudo random number techniques. Once the embedding process is completed, the inverse Haar DWT is applied in order to form the stego image. The vertical and horizontal operations are shown in Figure 1 and described briefly as follows [11].

2.1.1 Horizontal Operation

In this operation, an image will be divided into two bands that are low and high frequencies. Pixels are scanned from left to right in the horizontal direction. Addition and subtraction operations are performed on the neighboring pixels. The results of addition are on the left side that represents the low frequency band. However, subtraction, which represents the high frequency band, is held on the right side, as illustrated in Figure 1 (a).

2.1.2 Vertical Operation

Low and high frequencies obtained from the horizontal operation are further sub-divided into low-low, low-high, high-low and high-high frequencies. All pixels will be scanned over for the addition and subtraction operations, but in the vertical direction. The addition of the neighboring pixels will be held in the top, while the subtraction result will be located in the bottom, as illustrated in Figure 1 (b).

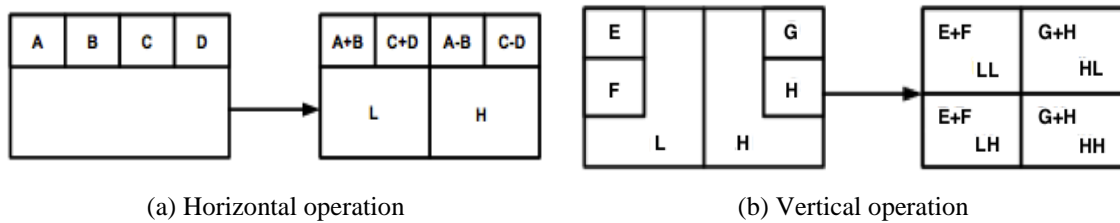


Figure 1. Horizontal and vertical operations.

2.2 LSB Technique

Least significant bit (LSB) is one of the common techniques being used for embedding data. It operates by replacing the least significant bit on one byte by another bit of a secret data. Images are made up of a large number of dots known as pixels and each pixel contains three bytes represented as RGB. Relying on the abundance of each colour, these three bytes will design the various colours of each pixel in the image that will result in changing the whole image colour. For example, the decimal RGB values for the black colour are (0, 0, 0), respectively. In contrast, the decimal RGB values for the white colour are (255, 255, 255). Table 1 shows that as the number of bytes changes, the colour of the pixel will be changed, which will result in changing the colour of the whole image. Furthermore, the range of colour for one byte will be from 0 to 255; that are from black to white.

Table 1. Resultant pixel colour relying on the abundance of each RGB.

	Red Layer (R)	Green Layer (G)	Blue Layer (B)	Resultant Colour
Binary	00000000	00000000	00000000	Black
Decimal	0	0	0	Black
Binary	11111111	11111111	11111111	White
Decimal	255	255	255	White

Changing the least significant bit-plane of one byte will not cause a visible effect on the overall colour of the pixels. The embedding process of the least significant bit technique will therefore replace the least significant bit of the cover medium with the secret data bits. Table 2 shows the effect on the overall colour of the pixel by altering the least significant bit of the cover image. It can be seen that the overall colour of the pixel will remain constant, even if the LSB has been changed. Therefore, hiding the bits of the secret data into the least significant bit of the cover image will not catch the attention of the eavesdroppers.

Table 2. Effect on the final colour of the pixel by changing LSB.

	Red Layer (R)	Green Layer (G)	Blue Layer (B)	Resultant Colour
Binary	10100101	00101010	00101010	Brown
Decimal	165	42	42	Brown
Binary	10100100	00101011	00101011	Brown
Decimal	164	43	43	Brown

2.3 Pseudo Random-Number Technique

In this technique, the secret image is embedded and extracted by a conventional way. The secret image is initially converted into binary representation and resized according to the cover image size in order to be concealed. When the coefficients of the secret image equal 0, a pseudo-random number will be added to the coefficients of the cover image. However, when the secret image equals 1, the cover image will be kept as it is. Nevertheless, at the decoder side, a correlation theory will be implemented in which the original cover image is compared to the stego image. If the coefficients of the stego image equal the coefficients of the original cover image, the value of the secret image will be 1; otherwise, it will be 0. The embedding (or encoding) and extracting (or decoding) process can be explained by the following examples.

Example 1: Embedding process

$$\text{Secret image} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{Cover image} = \begin{bmatrix} 10 & 13 \\ 11 & 14 \end{bmatrix} \quad \text{Stego-image} = \begin{bmatrix} 11 & 13 \\ 12 & 14 \end{bmatrix}$$

Example 2: Extracting process

$$\text{Stego image} = \begin{bmatrix} 11 & 13 \\ 12 & 14 \end{bmatrix} \text{ compares to Cover image} = \begin{bmatrix} 10 & 13 \\ 11 & 14 \end{bmatrix}$$

$$\text{Secret image} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

3. STEGANOGRAPHY ALGORITHMS

The algorithms presented in this section were designed and developed using MATLABTM environment. Details of the embedding and extraction algorithms of the proposed steganography are described as follows.

3.1 Embedding Algorithm

Figure 2 shows a block diagram for the proposed embedding process of hiding multiple types of information. Steps of the encoding process can be summarized as follows.

Step 1: Select and read cover image, three secret B&W images, one secret colour image and one secret text file.

Inputs: Cover image, three B&W secret images, one coloured secret image and one secret text file.

Process: The user will be asked to choose the cover image, three B&W secret images, one secret colour image and one secret text file in order to be read.

Outputs: Cover image, three B&W secret images, one coloured secret image and one secret text file are read.

End

Step 2: Separate cover image into three planes R, G and B.

Input: Cover image.

Process: Firstly, cover image will be resized to 512×512. After that, planes of the cover image will be separated into three layers that are red, blue and green. These layers will be used to hide various secret data.

Outputs: Separated cover image planes.

End

Step 3: Corrections of R, G and B planes of the cover image.

Inputs: Separated cover image planes.

Process: Firstly, Wavelet transform will be applied to the red-plane where the coefficient sizes excluding approximation will be determined. Secondly, green-plane will be converted into binary vector. Finally, B-plane will be reshaped, and then each pixel will be reduced by one bit.

Outputs: Separated cover image planes corrected.

End

Step 4: Correction of the secret data.

Inputs: Three B&W images, one secret colour image and one secret text file

Process: Firstly, B&W images will be resized according to horizontal, vertical and diagonal coefficients of the R-plane of the cover image. Secondly, secret colour image will be resized to 145 × 150, then reshaped into binary vector. Finally, secret text file will be converted into binary vector. After that, the length of this binary vector will be equalized according to the length of the B-plane of the cover image.

Outputs: Secret data corrected.

End

Step 5: Hide three B&W secret images into red layer.

Inputs: Red layer of the cover image.

Process: Three B&W secret images will be concealed within the red layer of the cover image using the techniques discussed in Section 2.

Output: Stego-red layer.

End

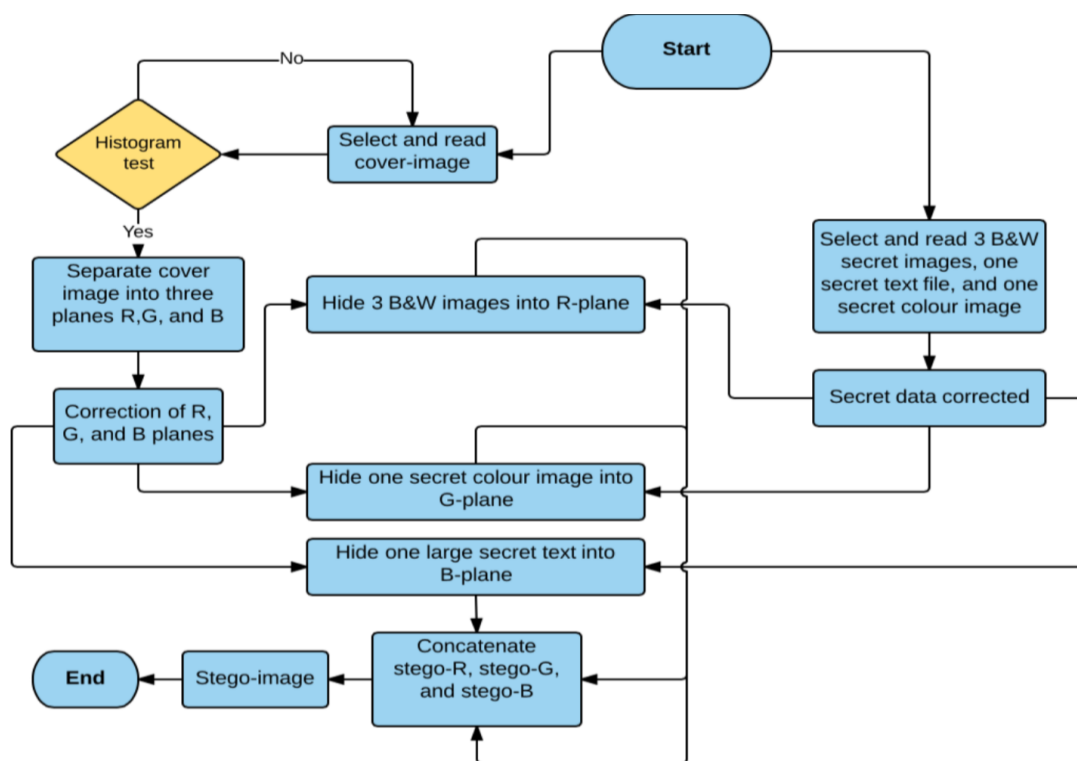


Figure 2. Encoding process of hiding multiple types of information [5].

Step 6: Hide one secret colour image into the blue layer.

Input: Blue layer.

Process: One secret colour image will be concealed within the blue layer.

Output: Stego-blue layer.

End

Step 7: Hide large secret text file into the green layer.

Input: Green layer.

Process: Following the same process that has been applied in step 5, the secret text file can be hidden within the green layer of the cover image.

Output: Stego-green layer.

End

Step 8: Concatenating three stego-layers together in order to create the stego image.

Inputs: Stego-red, Stego-blue and Stego-green layers.

Process: Stego-layers that are carrying various data will be concatenated in order to produce the stego image.

Outputs: Stego image.

End

3.2 Extraction Algorithm

Figure 3 shows a block diagram for the proposed extraction process of hiding multiple types of information. Steps of this process can be summarized as follows.

Step 1: Select and read stego and cover images.

Inputs: Stego and cover images.

Process: The user will be asked to select stego and cover images in order to be read.

Outputs: Stego image and cover image are read.

End

Step 2: Separation of the layers of stego and cover images.

Inputs: Stego-image and cover image.

Process: Stego and cover image layers will be separated into three layers that are R, G and B.

Outputs: Separated layers of the stego and cover images.

End

Step 3: Correction of the layers of stego and cover images.

Inputs: Separated layers of the stego and cover images.

Process: Firstly, Haar Wavelet transform will be applied to the R-layer of the stego and cover images in order to figure out the horizontal, vertical and diagonal coefficients. Secondly, the blue layer of the stego image will be converted into binary vector. Finally, Both green layers of the stego and cover images will be reshaped to 1D.

Outputs: Layers of the stego and cover images are corrected.

End

Step 4: Retrieving process of three B&W secret images.

Inputs: Horizontal, vertical and diagonal coefficients of the R-planes.

Process: Compare the horizontal coefficient of the stego image with the equivalent coefficient of the cover image. Using the pseudo random number technique, the secret binary image concealed within this coefficient can be retrieved. Similar process will be applied to the rest of the coefficients in order to extract other secret images.

Outputs: Three B&W secret images.

End

Step 5: Extraction process of one secret colour image.

Inputs: The blue layer of the stego image in binary vector.

Process: Secret colour image can be extracted by the use of least significant bits (LSB) technique. Binary vector can be obtained by taking two bits every 6 bits of the blue layer of the stego image in binary vector. Then, this binary vector will be divided into three equivalent binary vectors. Finally, these three binary vectors will be converted into 2D and concatenated in order to figure out the secret colour image in 2D format.

Outputs: One secret colour image.

End

Step 6: Extraction process of large secret text file.

Inputs: Reshaped green layers of the stego and cover images.

Process: Implementing pseudo random number techniques, the reshaped stego and cover image pixels will be compared in order to figure out a binary vector. This binary vector will be converted into a string of characteristics and saved as 'secret text file.txt'.

Output: Large secret text file.

End

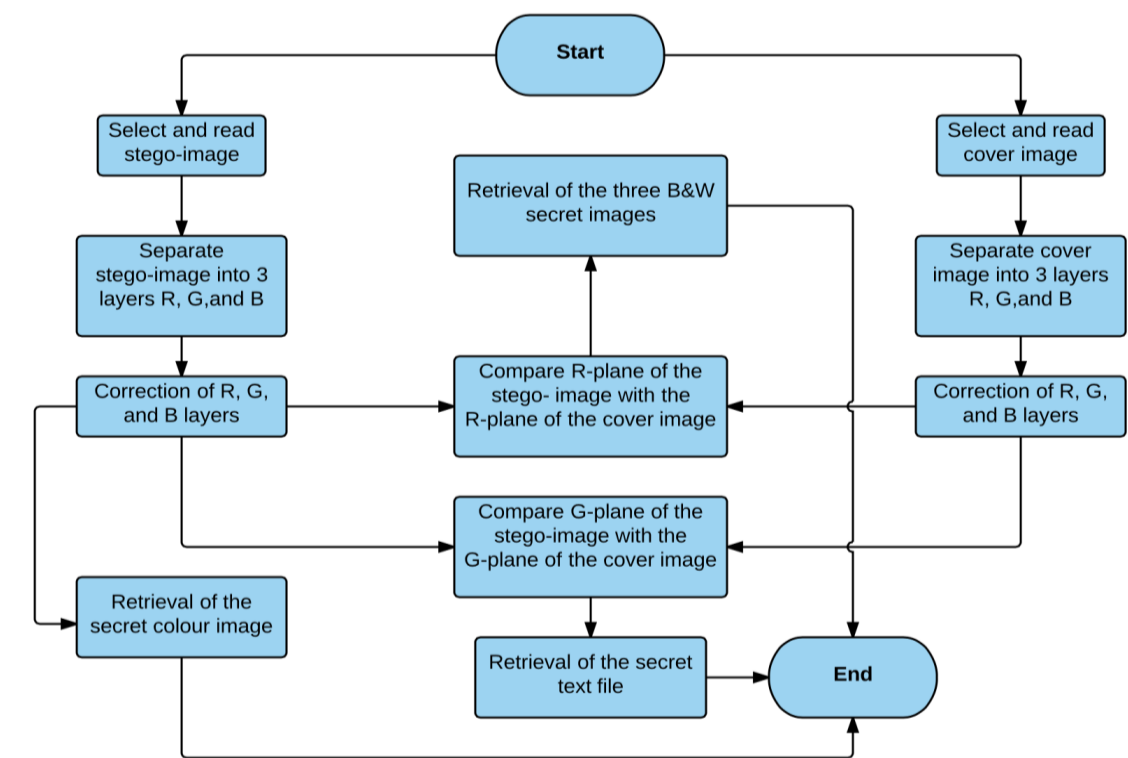


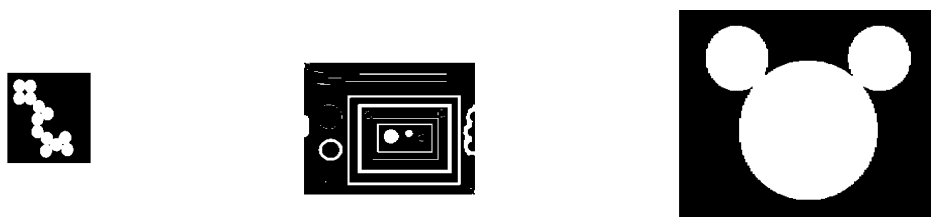
Figure 3. Decoding process of hiding multiple types of information [5].

4. DATA HIDING SCENARIOS

Scenarios of hiding different combinations of data types in a single cover image are presented and discussed in this section. These include hiding colour images, B&W images and larger text files or combinations of these data types in a single cover image.

4.1 Multiple B&W Images

In this scenario, the user can hide multiple B&W images as shown in Figure 4. The B&W images illustrated in Figure 4 (a) are embedded in a single cover image (Sailboat.tif), see Figure 4 (b). The obtained stego image is shown in Figure 4 (c). As illustrated, the stego image is indistinguishable from the original cover by the naked eye. Furthermore, the size of the stego image is identical to that of the original cover.



(a) Example of secret binary images

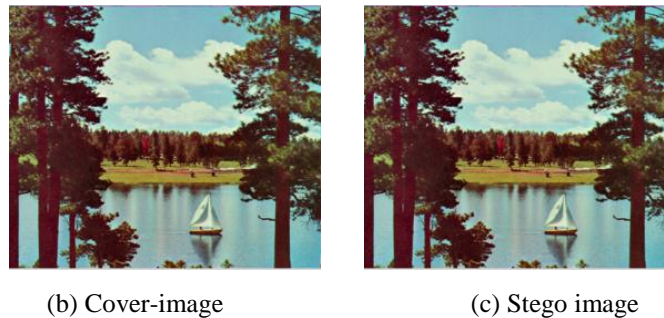


Figure 4. Hiding multiple B&W images in a single cover image (Sailboat.tif).

4.2 Multiple Coloured Images

In this scenario, the user can hide multiple coloured images as shown in Figure 5. The three coloured images of Figure 5 (a) are embedded in a single coloured image (Goldhill.bmp), see Figure 5 (b). In this case, two layers are used to hide the two images; each layer carries one secret colour image. As shown in Figure 5 (c), the resultant stego image is again indistinguishable from the original cover.



(a) Examples of secret coloured images



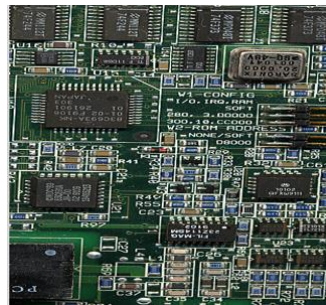
Figure 5. Hiding multiple coloured images in a single cover image (Goldhill.bmp).

4.3 Multiple Text Files

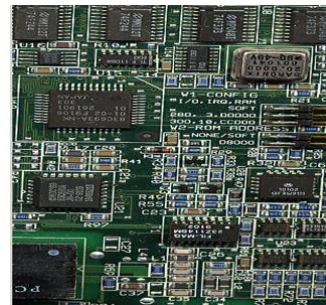
In this scenario, layers of the cover image are used to hide large text files. Figure 6 shows an example of hiding three copies of Shakespeare's *Tempest* (Figure 6 (a)) in a single cover image (board.tif) shown in Figure 6 (b). Each layer of the cover image carries one secret file. As illustrated, the appearance and size of the stego image of Figure 6 (c) are indistinguishable from those of the original image. It should be noted here that the size of each *Tempest*'s file comprises 107520 characters; hence more than 322000 characters can be concealed in a single cover image of a size of $512 \times 512 \times 3$ pixels.



(a) Secret text files (Shakespeare's Tempest text) [26]



(b) Cover image

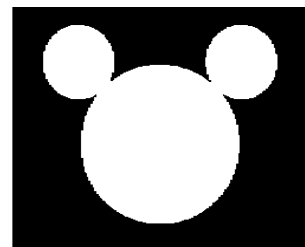
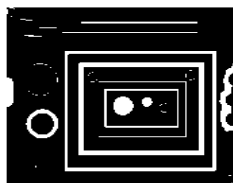
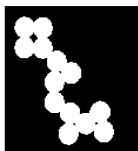


(c) Stego image

Figure 6. Hiding multiple text files in a single cover image (board.tif).

4.4 Miscellaneous Data Types

Figure 7 shows an example of hiding miscellaneous data types (i.e., B&W and coloured images and a large text file) in a single cover image (Lena.bmp). Figures 7 (d) and (e) depict the original cover and stego images, respectively. In this example, the size of the stego image is identical to that of the cover image, as illustrated.



(a) Example of secret binary images



(b) Secret coloured image



(c) Large text file



Figure 7. Hiding miscellaneous data in a single cover image (Lena.bmp).

5. PERFORMANCE EVALUATION

There are a various metrics that can be used in order to evaluate the performance of various steganography methods. In this paper, a number of performance evaluation metrics are used to evaluate the capacity (payload size) and imperceptibility of the cover image, as well as the robustness against various attacks. Measuring the PSNR and MSE assesses the imperceptibility, while measuring the correlation factor between the original and extracted secret images, after attacking the stego image by various noise attacks, assesses the robustness.

5.1 Capacity (Payload Size)

There is no specific definition for the capacity of the cover image. However, there are a various number of capacity expressions that can be used relying on different steganography approaches. In this paper, the capacity (C) has been defined as the amount of the cover image used for the embedding purpose [22].

$$C(\%) = \frac{\text{Pixels used for embedding purpose}}{J(i,j)} \times 100\% \quad (1)$$

where $J(i,j)$ represents the total rows and columns of the cover image (i.e., total number of the cover image pixels).

5.2 PSNR

Power signal-to-noise ratio is a measure of the difference between the original cover image and the stego image. It can be mathematically expressed as:

$$PSNR = 10 \times \log_{10}\left(\frac{n^2}{MSE}\right) \quad (2)$$

where n is the maximum pixel value for 8 bits.

5.3 MSE

Mean square error can be defined as the average square error between the cover image and the stego image. The mathematical expression for the MSE is given by:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^m \sum_{j=1}^n [J(i,j) - J'(i,j)]^2 \quad (3)$$

where $J(i,j)$ represents the cover image dimensions and $J'(i,j)$ represents the dimensions of the stego image.

6. RESULTS AND DISCUSSION

This section presents and discusses the results obtained from various experiments that were carried out to evaluate the imperceptibility of the stego image against different payload sizes for hiding various combinations of data types. It also presents some results on the robustness of the proposed algorithm against various kinds of attack.

6.1 Imperceptibility/Capacity Evaluation for Hiding Multiple B&W Images

Table 3 shows the performance evaluation when 3 B&W secret images are concealed within a single cover image. Various cover images with different formats such as .bmp and .tif have been used to demonstrate the efficiency of this algorithm. Moreover, there will be a small variation in the PSNR and the MSE, since the capacity is almost constant.

Table 3. Performance of hiding 3 logical images using various cover images.

Cover Image	PSNR (dB)	MSE	Capacity (%)
Lena.bmp	55.83	0.169	75
Goldhill.bmp	55.82	0.170	75
Sailboat.tif	55.78	0.171	75
Board.tif	55.96	0.164	75

6.2 Imperceptibility/Capacity Evaluation for Hiding Multiple Coloured Images

Table 4 shows the PSNR, MSE and capacity when hiding three coloured images. This algorithm has high capacity; hence the value of the PSNR will be decreased, while that of the MSE will be increased. Therefore, as the capacity increases, the PSNR and the MSE will be affected. Various image formats have been implemented and provided almost the same results as demonstrated.

Table 4. Performance of hiding 3 secret coloured images using various cover images.

Cover image	PSNR (dB)	MSE	Capacity (%)
Lena.bmp	43.70	0.925	99.56
Goldhill.bmp	43.90	0.882	99.56
Sailboat.tif	43.90	0.882	99.56
Board.tif	43.90	0.882	99.56

6.3 Imperceptibility/Capacity Evaluation for Hiding Multiple Text Files

Table 5 shows how the PSNR and the MSE are changing when the capacity increases. As the text entered by the user increases, the PSNR will be decreased, while the MSE will be increased. For example, when the number of bits is equal to 840; that is equal to 120 text letters, the PSNR and the MSE are equal to 80.74 dB and 0.00055, respectively. However, when the number of the embedded bits is equal to 752640, which is equivalent to 107520 text letters, PSNR and MSE are equal to 51.30 dB and 0.8233, respectively. Figures 8 and 9 illustrate clearly the relation between the capacity and PSNR, as well as the relation of the capacity and MSE, respectively.

From Figure 8, it can be seen that the PSNR drops with the increase of the payload (size of message to be hidden with respect to the total cover medium size). In fact, this is typical, but increasing the payload from about 100 Kbit to about 700 Kbit will result in a drop of the PSNR of about 10 dB; a drop that is basically not huge. This illustrates the effectiveness of the proposed algorithm. Same conclusion can be drawn from Figure 9, where the MSE increases (from about 0.05% to approximately 0.45%) when the payload goes up by the same amount mentioned above.

Table 5. Performance of hiding various sizes of secret text.

Cover Image	PSNR (dB)	MSE (%)	Embedded Text Size (Kbits)
Sailboat.tif	80.74	0.00055	0.840
Sailboat.tif	77.73	0.00109	1.680
Sailboat.tif	74.71	0.00219	3.360
Sailboat.tif	71.68	0.00442	6.720
Sailboat.tif	68.66	0.00885	13.440
Sailboat.tif	65.65	0.01769	26.880
Sailboat.tif	62.64	0.03539	53.760
Sailboat.tif	59.63	0.07079	107.520
Sailboat.tif	56.83	0.13495	215.040
Sailboat.tif	53.82	0.26992	430.080
Sailboat.tif	51.30	0.48233	752.640

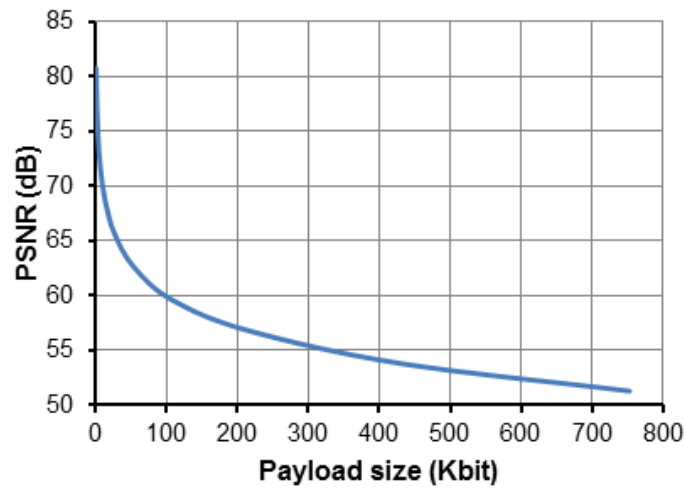


Figure 8. PSNR against payload size for hiding private text.

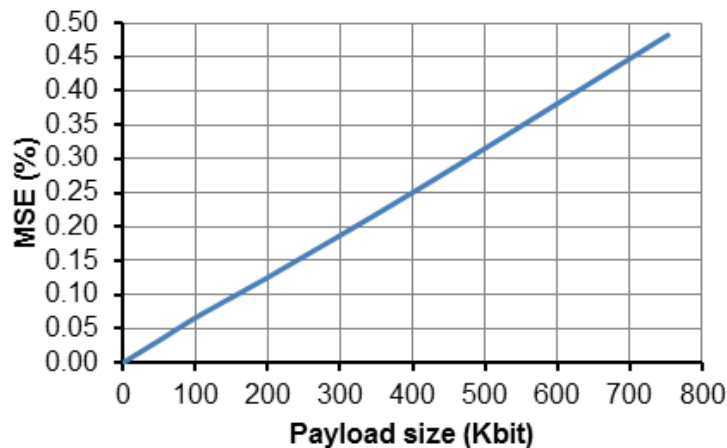


Figure 9. MSE against capacity for hiding private text.

6.4 Imperceptibility/Capacity Evaluation for Hiding Miscellaneous Data Types

Table 6 shows the values of the PSNR and the MSE when hiding multiple types of private data. It can be seen that as the capacity increases, MSE and PSNR will be affected. Figures 10 and 11 show how the capacity affects the PSNR and the MSE, respectively.

Table 6. Performance of hiding multiple private data.

Cover Image	PSNR (dB)	MSE (%)	Embedded Data Size (Kbits)
Sailboat.tif	48.180	0.32950	719.448
Sailboat.tif	48.178	0.32973	720.288
Sailboat.tif	48.173	0.33001	721.968
Sailboat.tif	48.163	0.33084	728.328
Sailboat.tif	48.144	0.33232	732.008
Sailboat.tif	48.106	0.33527	745.488
Sailboat.tif	48.010	0.34117	772.368
Sailboat.tif	47.881	0.35297	826.128
Sailboat.tif	47.625	0.37435	933.648
Sailboat.tif	47.524	0.38320	973.968

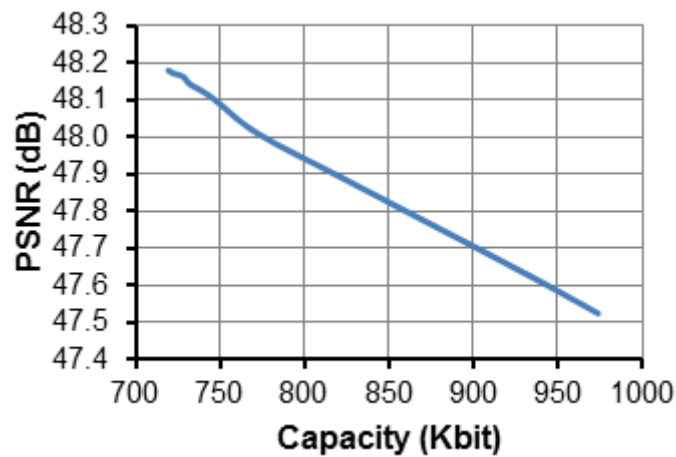


Figure 10. PSNR against capacity for hiding multiple types of private data.

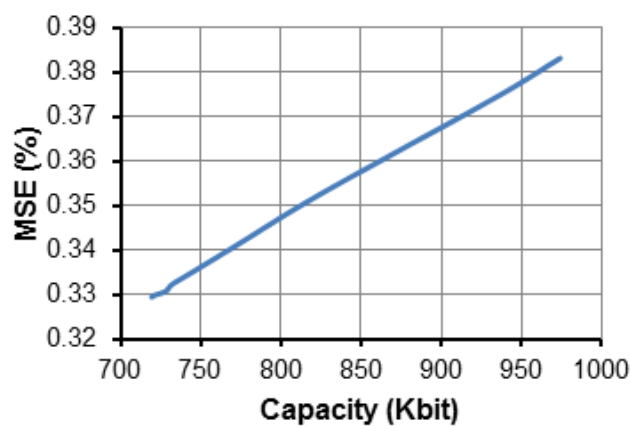


Figure 11. MSE against capacity for hiding multiple types of private data.

The proposed steganography techniques provide not only high capacity, but also high PSNR and low MSE. The size of the concealed secret text file (i.e., Shakespeare's *Tempest*) equals about 752640 bits which is equivalent to 107520 letters. Moreover, sizes of the stego image formed in all the proposed techniques were equal to the size of the cover image, which is 512×512×3 pixels. Capacity values are found to be high except for that of hiding B&W images,

since the approximation coefficients that represent the low-low frequencies of the Wavelet transform have not been used for the hiding process. However, as the capacity increases, PSNR decreases and MSE increases. Table 7 summarizes the obtained performance parameters for the developed algorithm.

Table 7. Performance summary.

Hidden Data	PSNR (dB)	MSE (%)	Capacity (%)
Multiple data	47.52	0.383	89.42
3 B&W images	55.78	0.171	75
3 Colour images	43.93	0.877	99.56
Text file	51.43	0.467	95.70

Embedding three binary secret images within a single cover image by the use of Wavelet transform has been proposed and successfully implemented. The PSNR, MSE and capacity achieved in this technique were found to be equal to 55.78 dB, 0.171 and 75%, respectively. Moreover, another technique has also been proposed, where the user will have the ability to hide a single secret colour image within one cover image. PSNR, MSE and capacity are equal to 43.93 dB, 0.877 and 99.56%, respectively. Another technique to hide large secret text files was also proposed. The capacity in this technique can vary depending on the size of the secret text file. However, the results of hiding large pdf files have been presented. Furthermore, a method to conceal three binary images, one secret colour image and one large text file has been suggested in this paper. Figures 10 and 11 illustrate the effect of the payload size on the PSNR and the MSE, respectively.

6.5 Robustness Evaluation for Hiding Miscellaneous Data Types




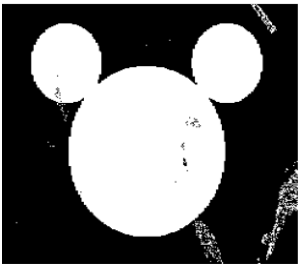
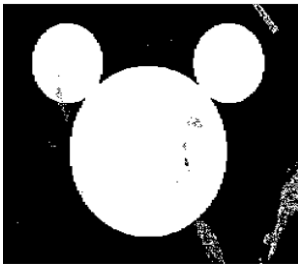
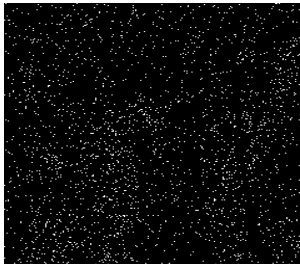



Robustness of the proposed steganography algorithm is tested through embedding miscellaneous secret data (i.e., three B&W images, a coloured image and a text file) in a cover (Lina image). The obtained stego image shown in Figure 12 is then exposed to Gaussian with white noise, Poisson noise, and salt and pepper noise. The attacked stego images and the miscellaneous secret data retrieved from each of the attacked images are summarized in Table 8.



Figure 12. Original stego image.

The obtained results clearly demonstrate that the robustness of the developed steganography algorithm varies depending on the type of the embedded data and the type of attack. For example, it is shown that unlike B&W images, colour images and texts are not affected by the attacks used in this study. Furthermore, B&W images are only slightly distorted by the Gaussian with white noise and Poisson noise attacks, but are found fragile against salt and pepper noise attacks. The correlation between the original and the extracted secret images is measured and presented in Table 9. It should be mentioned here that the correlation factor measurement that is applied to evaluate robustness of the secret images is not applicable to secret text files.

Table 8. Summary of robustness tests against various attacks

	Gaussian with white noise	Poisson noise	Salt and pepper noise
Attacked stego image			
Retrieved secret B&W image			
Retrieved secret coloured image			
Retrieved secret B&W text	<p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p>	<p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p>	<p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p> <p>William Shakespeare (1564 - 1616) was born at Stratford-upon-Avon in a house in Henley Street. This is preserved intact.</p>

The nature of salt and pepper noise is to affect the B&W pixels; hence the binary images are highly affected by this kind of noise. In addition, the adopted pseudo random numbers that are dependent on the B&W pixels also affect concealing B&W images. Partial or total distortion is therefore expected on the canceled B&W images when exposed to salt and pepper noise due to the fact that pixels of such images have binary values that are easily corrupted with a probability value of 50%. However, the effect of this noise can be reduced by the use of median or morphological filters. Nevertheless, as discussed earlier in the introduction, robustness in steganography is less important than in watermarking, since the attacker is mainly concerned with the discovery of hidden data rather than with removing or modifying them.

Table 9. Correlation factor measurement for various types of attacks.

	Gaussian with white noise	Poisson noise	Salt and pepper noise
Colour image	1	1	1
B&W image (blobs.png)	1	1	0.20
B&W image (Circles.png)	1	1	0.25
B&W image (Binary_circles.png)	1	0.997	0.06
B&W text	N/A to secret texts		

7. CONCLUSION

In this paper, a high-capacity image steganography algorithm based on Haar wavelet transform that is capable of hiding various data types (i.e., B&W and coloured images, as well as text files) has been presented. All these types of private data are concealed in stego images of a unified size of $512 \times 512 \times 3$ pixels. The stego image is formed to be always equal to the cover image. Experimental evaluation has proven that the proposed steganography is highly efficient in terms of capacity size of the cover image while maintaining a relatively low MSE and high PSNR and is reasonably robust against external attacks. The provided results have confirmed this conclusion.

The developed algorithms can also be further improved by the use of Huffman coding in order to have more area for hiding extra data; hence increasing the capacity. Moreover, robustness, which can be defined as how long the stego carrier can withstand before an eavesdropper can extract the concealed data, is another area for future improvement. For example, the binary vector of the secret image can be divided into a number of small blocks where each block can then be concealed randomly within the cover image. Thus, even if eavesdroppers discover the stego image, they will not have the ability to assemble the hidden blocks of the secret image. Cryptography can also be added to improve security through allocating unused pixels for cryptography bits. These potential improvements among others are currently part of the ongoing research of the authors. Also, measures for image quality assessment like structural similarity index (SSI) or structural similarity index mean (SSIM) can be used to assess the quality of data embedding.

Finally, steganography is an open area for further research, as many algorithms can still be proposed and practically implemented. However, it is worth mentioning that security, robustness and payload (capacity) will always conflict with each other. A fourth factor that can be added here is the performance or algorithm execution time that can add more challenge in this research area.

REFERENCES

- [1] H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study," Journal of Global Research in Computer Science, vol. 3, no. 12, pp. 33-35, 2012.
- [2] M. A. Al-Tae, N. H. Al-Hassani, B. S. Bamajbour and D. Al-Jumeily, "Biometric-Based Security System for Plaintext E-mail Messages," in: Proc. International Conference on Developments in eSystems Engineering, Abu Dhabi, UAE, , pp. 1-6, 14 – 16 December 2009.
- [3] N. Qasrawi, M. A. Al-Tae, H. l'emair and R. Al-Asa'd, "Multilevel Encryption of Plaintext Messages Using a Smart Card Connected to PC Parallel Port," in: Proc. 3rd International

- Conference on Modelling, Simulation and Applied Optimization, Sharjah-UAE, , pp. 1-6, 20-22 January 2009.
- [4] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Inc, 2000.
 - [5] H. A. Al-Korbi, A. Al-Ataby, M. A. Al-Tae and W. Al-Nuaimy, "High-Capacity Image Steganography Based on Haar DWT for Hiding Miscellaneous Data," in: Proc. IEEE/AEECT'2015 Jordan Conference on Applied Electrical Engineering and Computing Technologies, Amman, Jordan, pp. 1-6, 3-5 November 2015.
 - [6] S. Jayasudha, "Integer Wavelet Transform Based Steganography Method Using Opa Algorithm," *International Journal of Engineering and Science*, vol. 2, no. 4, pp. 31–35, 2013.
 - [7] A. Al-Ataby and F. M. Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform," *International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 358–364, 2010.
 - [8] S. Banerjee, S. Chakraborty, N. Dey, A. K. Pal and R. Ray, "High Payload Watermarking Using Residue Number System," *International Journal of Image, Graphics and Signal Processing*, vol. 3, pp. 1-8, 2015.
 - [9] M. S. Al-Yaman, M. A. Al-Tae and H. Alshammas, "Audio-Watermarking Based Ownership Verification System Using Enhanced DWT-SVD Technique," in: Proc. IEEE/SSD2012 Multi-Conference on Systems, Signals and Devices, Chemnitz-Germany, pp. 1-5, 20-23 March 2012.
 - [10] M. S. Al-Yaman, M. A. Al-Tae, A. T. Shahrour and I. A. Al-Husseini, "Biometric Based Audio Ownership Verification Using Discrete Wavelet Transform and SVD Techniques," in: Proc. IEEE/SSD2011 Multi-Conference on Systems, Signals and Devices, Tunisia, pp. 1-5, 22-25 March 2011.
 - [11] N. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEE Computer*, vol. 31, pp. 26–34, 1998.
 - [12] D. Wu and W. Tsai, "A Steganography Method for Images by Pixel-value Differencing," *Pattern Recognition Letters*, vol. 24, pp. 1613–1626, 2002.
 - [13] A. Hashad, A. Madani and A. Wahdan, "A Robust Steganography Technique Using Discrete Cosine Transform Insertion," in: Proc. Int. Conf. on Information and Communications Technology, Cairo, Egypt, pp. 255–264, 5-6 December 2005.
 - [14] P. Chen and H. Lin, "A DWT Approach for Image Steganography," *International Journal of Applied Science and Engineering*, vol. 4, no. 3, pp. 275–290, 2006.
 - [15] H. S. Reddy and K. B. Raja, "High Capacity and Security Steganography Using Discrete Wavelet Transform," *International Journal of Computer Science and Security*, vol. 3, no. 6, pp. 462-472, 2010.
 - [16] N. Dey, A. Roy and S. Dey, "A Novel Approach of Colour Image Hiding Using RGB Colour Planes and DWT," *International Journal of Computer Applications*, vol. 36, no. 5, pp. 19–24, 2011.
 - [17] T. Bhattacharya, N. Dey and S. Chaudhuri, "A Session Based Multiple Image Hiding Technique Using DWT and DCT," *International Journal of Computer Applications*, vol. 38, no.5, pp. 18–21, 2012.
 - [18] E. Ghasemi, J. Shanbehzadeh and N. Fassihi, "High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm," in: Proc. Int. Multi-Conference of Engineering and Computer Scientists (IMECS), vol. 1, Hong Kong, pp. 1–4, 16-18 March 2011.
 - [19] S. Laskar and K. Hemachandran, "High Capacity Data Hiding Using LSB Steganography and Encryption," *International Journal of Database Management Systems*, vol. 4, no. 6, pp. 57–68, 2012.
 - [20] P. Ganesan and P. Bhavani, "A High Secure and Robust Image Steganography Using Dual Wavelet and Blending Model," *Journal of Computer Science*, vol. 9, no. 3, pp. 277–284, 2013.

- [21] M. Parul and R. Harish, "Optimized Image Steganography Using Discrete Wavelet Transform (DWT)," International Journal of Recent Development in Engineering and Technology, vol. 2, no. 2, pp. 75–81, 2014.
- [22] A. Nag, S. Biswas, D. Sarkar and P. Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, vol. 4, no. 6, pp. 561–570, 2011.
- [23] I. Badescu and C. Dumitrescu, "Steganography in Image Using Discrete Wavelet Transformation," in: Proc. WSEAS Conf. on Advances in Mathematical Models and Production Systems in Engineering, Brasov, Romania, pp. 69-72, 26-28 June 2014.
- [24] M. Sifuzzaman, M. Islam and M. Z. Ali, "Application of Wavelet Transform and Its Advantages Compared to Fourier Transform," Journal of Physical Science, vol. 13, pp. 121–134, 2009.
- [25] L. Jing, K. Zhi-wei and H. Yi-gang, "A Steganography Method Based on Wavelet Contrast and LSB," Chinese Journal of Electronics, vol. 35, pp. 1391–1393, 2007.
- [26] W. Shakespeare, "The Tempest," Online: <http://sparks.eserver.org/books/shakespeare-tempest.pdf>, last accessed 15 January 2016.

ملخص البحث:

أصبحت حماية البيانات الخاصة التي يجري تبادلها على الإنترنت ومن يمكنه الوصول إلى تلك البيانات أمراً بالغ الأهمية والضرورة لما ينطوي عليه من مسائل تتعلق بالخصوصية والسرية. ويساعد إخفاء الصور أو أجزاء منها في تحسين البيانات الخاصة داخل صورة غلاف للحصول على غلاف جديد لا يمكن عملياً تمييزه عن الغلاف الأصلي، بطريقة تمنع الأشخاص غير المخولين من كشف البيانات المحصنة في الغلاف الجديد. لذا؛ فإن سعة صورة الغلاف وانعدام قابليتها للإدراك يُعدّان من المتطلبات الحاسمة لتقويم أداء خوارزميات الإخفاء.

تقدم هذه الورقة خوارزمية إخفاء عالية الفعالية لها القدرة على إخفاء حجم كبير من البيانات المتفرقة؛ مثل ملفات النصوص، والصور الثنائية، والصور الملونة أو تركيبة من هذه الأنواع من البيانات، في صورة غلاف واحدة باستخدام تحويل "هار" للموجات. وقد تم عرض تفاصيل خوارزميات الإخفاء والاستخراج للأنواع المختلفة من البيانات ومناقشتها. وتم تقويم أداء طريقة الإخفاء المقترحة من حيث سعة صورة الغلاف، وانعدام قابلية الإدراك، والمتانة. وبينت النتائج والملاحظات التي تم الحصول عليها أن الخوارزميات التي جرى تطويرها ذات فعالية عالية من حيث سعة صورة الغلاف، مع الحفاظ على قيمة منخفضة نسبياً للخطأ التربيعي المتوسط وقيمة عالية لأعلى نسبة للإشارة إلى الضجيج، إضافة إلى متانة معقولة ضد الهجمات المختلفة.